



Veeam Backup & Replication with VMware Cloud on AWS

Deployment guide for data protection and disaster recovery through Veeam Backup & Replication v11 and VMware Cloud on AWS

Dustin Albertson

Manager of Cloud & Applications
Product Management,
Alliances

2021



© 2021 Veeam® Software. All rights reserved worldwide.

No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by electronic, mechanical, recording, photocopy, scanning or other means without prior written permission from Veeam Software.

The product described in this documentation may be protected by one or more U.S. patents or pending patent applications.

Veeam® Software has used the latest information that is available in producing this document. Veeam makes no warranty, expressed or implied, with regard to accuracy or completeness.

This documentation is provided "as is" and all express or implied conditions, representations and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Veeam shall not be liable for incidental or consequential damages in connection with the furnishing, performance or use of this documentation.

No portions of this document may be reproduced without prior written consent of Veeam Software. Specifications are subject to change without notice.

Information in this document is subject to change without notice.

Veeam is a trademark of Veeam Software.

All brand names and product names mentioned in this document are trademarks of their respective owners. Where known, trademarked, registered trademarks and service marks are designated as such.

Any other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without written permission from Veeam Software (Veeam). The information contained in this document represents the current view of Veeam on the issue discussed as of the date of publication and is subject to change without notice. Veeam shall not be liable for technical or editorial errors or omissions contained herein. Veeam makes no warranties, express or implied, in this document. Veeam may have patents, patent applications, trademark, copyright or other intellectual property rights covering the subject matter of this document. All other trademarks mentioned herein are the property of their respective owners. Except as expressly provided in any written license agreement from Veeam, the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.

Veeam Software Linden Park. Lindenstr. 16 Baar, Switzerland 6340

<https://www.veeam.com>

Revision 2.0

Contents

Contacting Veeam Software	4
Customer support	4
Online support	4
Company contacts	4
Introduction	5
Purpose	5
Intended audience	5
Solution overview	6
VMware Cloud on AWS and Veeam solutions – Better Together	6
Veeam overview	7
Validation	7
Compatibility	8
Deployment use cases	9
System requirements	16
Configuration	17
References	30
About Veeam Software	31

Contacting Veeam Software

At Veeam Software, we value feedback from our customers. It is not only important to help you quickly with technical issues, but it is also our mission to listen to your input and build products that incorporate your suggestions.

Customer support

Should you have a technical concern, suggestion or question, visit our Support Portal at <https://www.veeam.com/support.html> to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Online support

If you have any questions about Veeam solutions, you can use the following resources:

- Full documentation set at <https://www.veeam.com/documentation-guides-datasheets.html>
- Community forum at <https://forums.veeam.com>

Company contacts

For the most up-to-date information about company contacts and office locations, visit www.veeam.com/contacts.html.

Introduction

Purpose

This deployment guide is designed to assist administrators with the initial setup of Veeam Backup & Replication™ using VMware Cloud on AWS for backup and restore, specifically within the customer environment. Additional use cases, including multi-site deployments and off-site backup and disaster recovery will also be covered. This document will review multiple storage and connectivity options for connecting storage as a backup target. There are architectural considerations and sizing guidelines identified for general backup workloads.

Intended audience

This document is primarily aimed at solution architects, consultants, administrators and other IT professionals involved in deployment planning and implementation. An intermediate level of VMware virtual infrastructure and AWS knowledge as well as an advanced understanding (Veeam Certified Engineer [VMCE] level) of Veeam Backup & Replication are required.

Solution overview

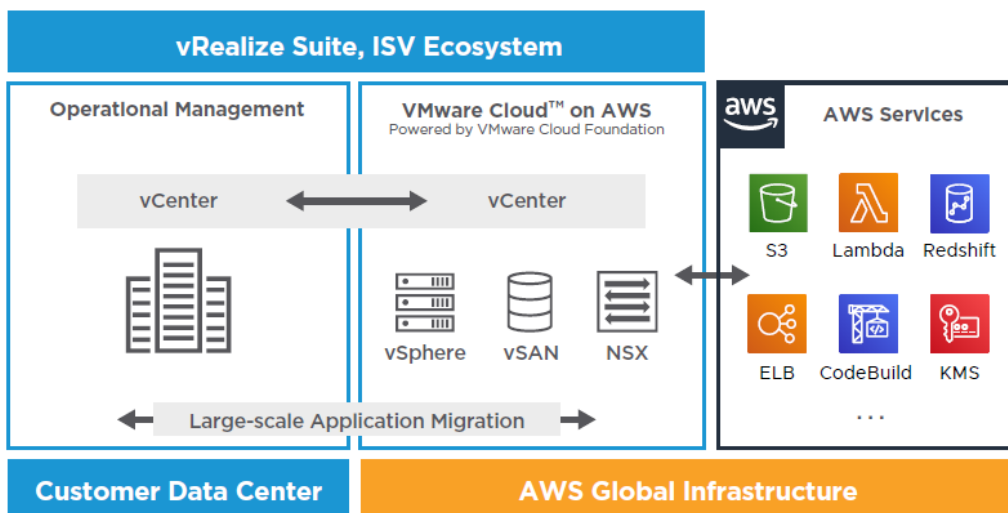
VMware Cloud on AWS and Veeam solutions – Better Together

VMware Cloud on AWS brings VMware's enterprise-class SDDC software to the AWS cloud with optimized access to native AWS services. Powered by VMware Cloud Foundation, VMware Cloud on AWS integrates VMware's compute, storage and network virtualization products (VMware vSphere, VMware vSAN and VMware NSX), along with VMware vCenter Server management, optimized to run on a dedicated, elastic and bare-metal AWS infrastructure.

With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant business value from use of the AWS and VMware hybrid cloud experience.

VMware Cloud on AWS

VMware vSphere-based service running on the AWS Cloud



AWS

AWS is a secure cloud services platform offering compute power, database storage, content delivery and other functionality to help businesses scale and grow. Explore how millions of customers are currently leveraging AWS cloud products and solutions to build sophisticated applications with increased flexibility, scalability and reliability.

In this scenario, AWS is used in the background to host the VMware Cloud on the AWS server, network and workloads. For backup, it provides the necessary backup target infrastructure.

Veeam overview

Veeam Backup & Replication™ is a comprehensive data protection and disaster recovery solution. With Veeam Backup & Replication, you can create image-level backups of virtual, physical and cloud machines and restore from them. Veeam provides support for VMware Cloud on AWS. With Veeam Backup & Replication, you can administer backup, replication and restore operations in VMware Cloud on AWS environments.

The major components of Veeam Backup & Replication consist of a management server, proxy servers, backup repository servers and disk-based backup repositories. The backup management server and backup proxy servers are Windows-based installations. The backup repositories can be Windows- or Linux-based, network attached storage systems or tape. These resources can be virtual or physical, depending upon the storage and network topology, desired throughput of backup and recovery data streams, as well as the available server resources.

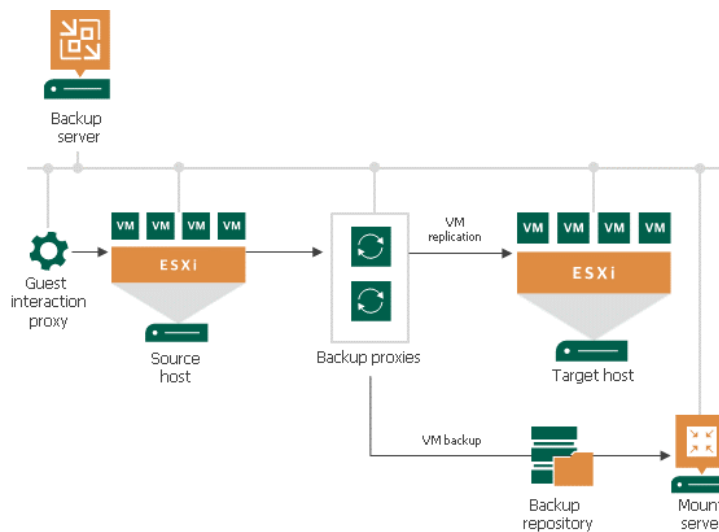


Figure 1 Veeam backup architecture

Validation

The following architectural components have been validated. For the latest listing, visit:

<https://www.veeam.com/kb2414>

Validated components

VMware Cloud on AWS: review the VMware Compatibility Guide (VCG) linked above

Veeam Backup & Replication v9.5 U3 or later (v11 preferred)

AWS Storage Gateway (VTL Mode)

Amazon Elastic File System (Amazon EFS)

Amazon FSx

Amazon S3

Amazon AWS EC2 Instance (C4 Instance type with Amazon EBS [Elastic Block Store] ST1 volume as the backup target)

Compatibility

Veeam KB entry for VMware Cloud on AWS compatibility: <https://www.veeam.com/kb2414>

For a description of these features, visit: <https://www.veeam.com/backup-replication-features.html>

Current limitations and workarounds

Affected Veeam feature	Limitation	Workaround
Instant VM Recovery®	Currently, VMware Cloud on AWS does not allow for NFS usage	Use a combination of a Veeam backup job and replication job for proactive restore capabilities
Other OS file level recovery	Currently, VMware Cloud on AWS does not allow for NFS	Start Linux File Level Recovery from a backup copy on-premises
SureBackup®, SureReplica, On-Demand Sandbox, Virtual Lab	Currently, VMware Cloud on AWS does not allow NFS and network manipulation	As for SureReplica, you can perform it if the replication target is a non-VMware Cloud on AWS vSphere environment (e.g., replicate VM from VMware Cloud on AWS to on-premises)
VM replication ReIP	ReIP is not available on VMware Cloud on AWS	
Non-Unicode VM names	Currently, VMware Cloud on AWS does not allow non-Unicode characters for VM names within their APIs	
VM replication-based file-level recovery		Use file restore from backups or use a VM replica on a non-VMware Cloud on AWS environment to start file recovery
Replication (where EC2-based repository is used to store replica metadata)	Due to the lack of permissions, the repository Data Mover is not able to connect to the Veeam server	Enable Run server on this side option for the repository. For Windows repositories, it can be found under Ports configuration , for Linux, under Advanced settings in the server configuration wizard.

Note: At the time of writing, the above current limitations and workarounds apply. Please consult KB2414 above for the most recent updates.

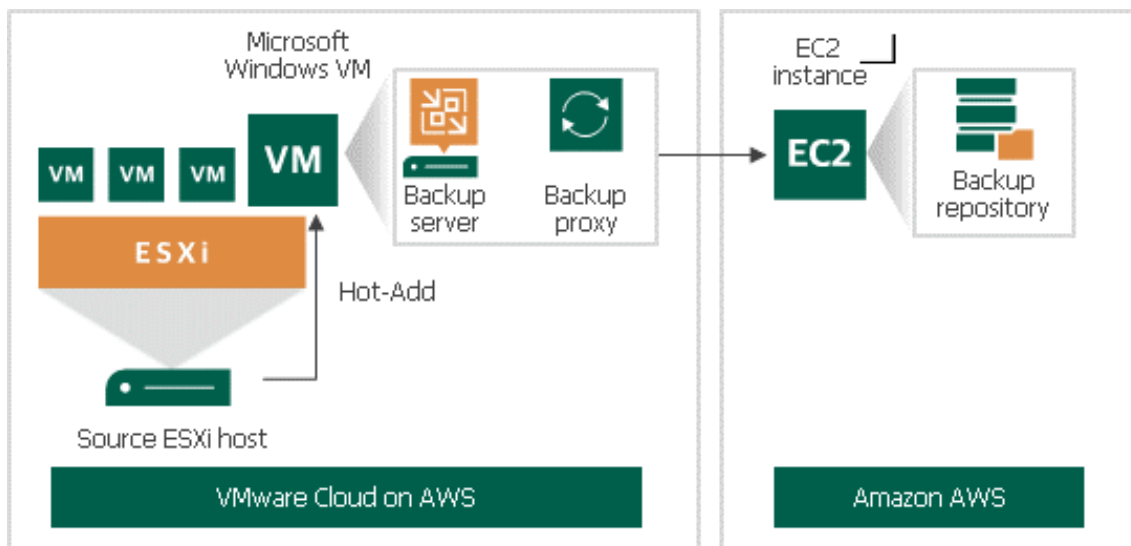
Deployment use cases

This section will examine a few of the deployment use cases for Veeam Backup & Replication in VMware Cloud on AWS, as well as ways to meet the 3-2-1 Rule for data availability.

Simple deployment

Simple deployment is preferable for VMware Cloud on AWS environments with a low traffic load. Per this deployment type, you can install the backup server and the backup proxy on the same virtual machine. In a simple VMware Cloud on AWS deployment, the backup infrastructure includes the following components:

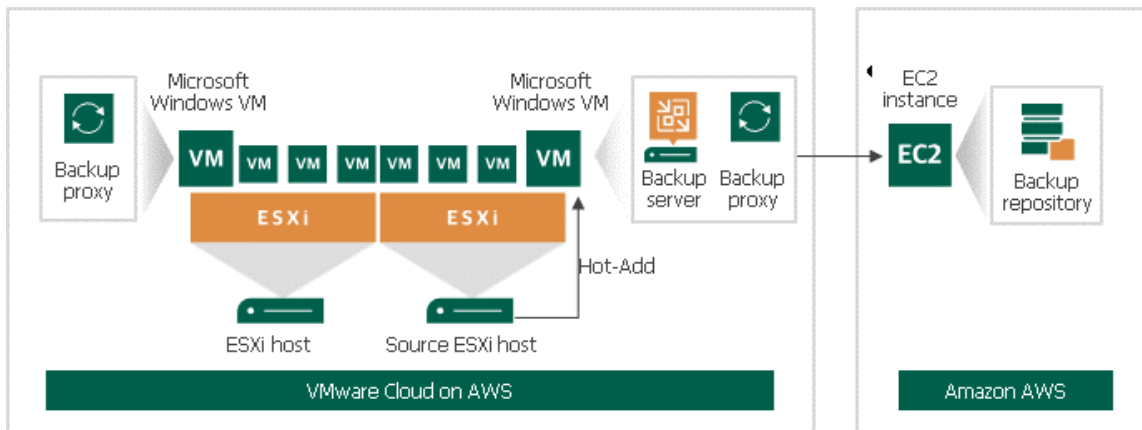
- Source ESXi host(s) of the VMware Cloud on AWS
- VMware to Amazon EC2 Elastic Network Interface (ENI).
- Veeam Backup Server (includes Veeam proxy)
- Veeam Backup Repository: a Linux-based EC2 instance in Amazon AWS
- Veeam Cloud Connect or AWS Storage Gateway in VTL Mode (refer to section on off-site backups)



Advanced deployment

Advanced deployment is intended for large-scale VMware Cloud on AWS environments with a large number of backup and replication jobs. Per this deployment type, it is recommended to install several backup proxies on dedicated virtual machines to move a workload from the backup server. In an advanced VMware Cloud on AWS deployment, the backup infrastructure includes the following components:

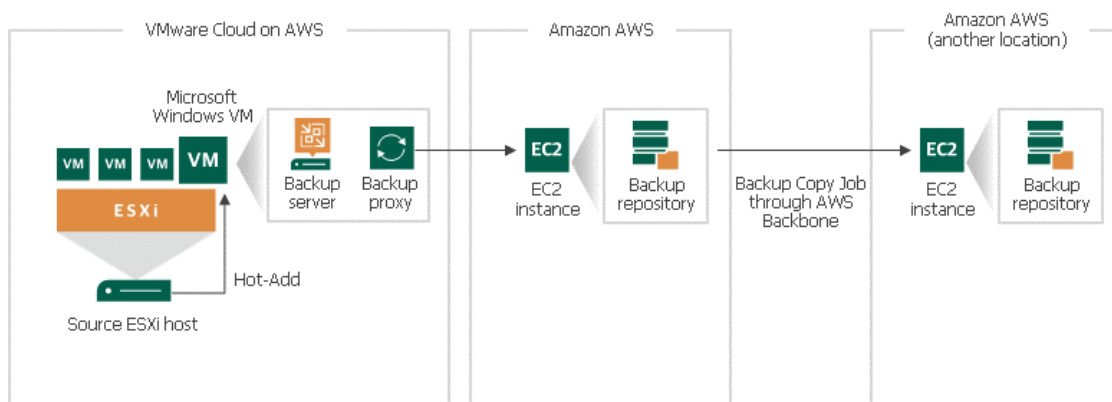
- Source ESXi host(s) of the VMware Cloud on AWS
- VMware to Amazon EC2 Elastic Network Interface (ENI)
- Veeam Backup Server (include Veeam proxy)
- Several Veeam Backup Proxies for better performance and workload distribution
- Veeam Backup Repository: a Linux-based EC2 instance in Amazon AWS
- Veeam Cloud Connect or AWS Storage Gateway in VTL Mode (refer to section on off-site backups)



Deployment scenarios for off-site backup Secondary region option

As mentioned above, to maintain the 3-2-1 Rule for backup, it is recommended that you have a copy of your backup in an off-site location. To transfer your backup off site, you can leverage Veeam backup copy jobs. The examples below will work with both a simple and advanced deployment model and that the images used are leveraging the simple model for illustration purposes only. Transferring backups over the internet may incur a charge for outbound data transfer. As a cost-effective alternative, you can store backups in a different Amazon AWS region. In this case, backup copies are transferred through the AWS backbone. Using this AWS network solution provides data transfer at lower latency and cost compared to the public internet. To transfer a backup copy to a different Amazon AWS region, the backup infrastructure must contain the following components:

- Source ESXi host(s) of the VMware Cloud on AWS
- VMware to AWS EC2 Elastic Network Interface (ENI)
- Veeam Backup Server
- Veeam Backup Proxy
- Veeam Backup Repository: a Linux-based EC2 instance in Amazon AWS
- Veeam Backup Repository for a backup copy: a Linux-based EC2 instance in another Amazon AWS region

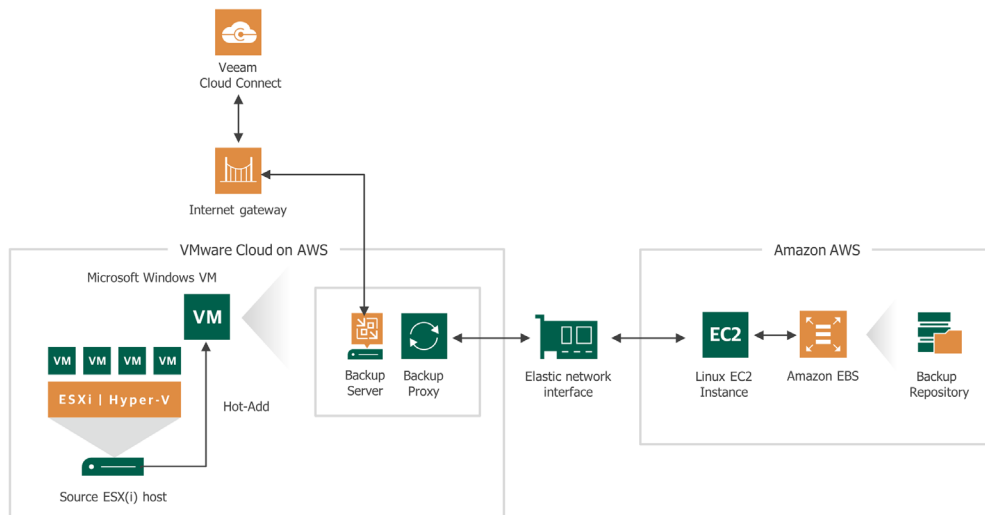


Deployment scenarios for off-site backup

Veeam Cloud Connect option

In this case, backup copies are transferred through the public internet. Note that this use case may incur outbound data transfer charges. To perform a backup copy to a Cloud Connect location, the backup infrastructure must contain the following components:

- Source ESXi host(s) of the VMware Cloud on AWS
- VMware to AWS ENI Network Tunnel
- Veeam Backup Server
- Veeam Backup Proxy
- Veeam Backup Repository: a Linux-based EC2 instance in Amazon AWS
- Veeam Cloud Connect repository for a backup copy



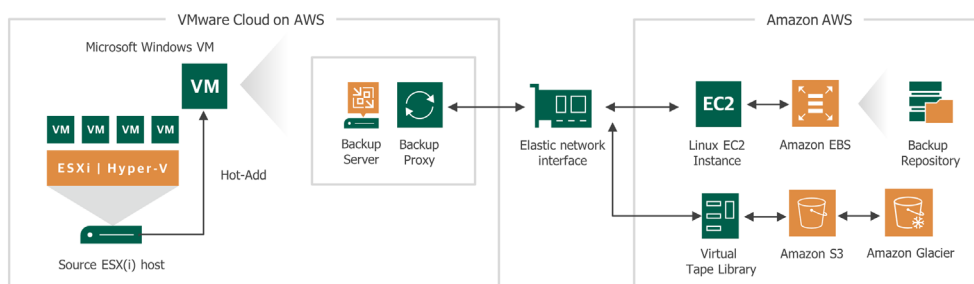
Deployment scenarios for off-site backup

VTL option

In this case, backup copies are transferred through the AWS backbone. Using such an AWS network solution provides data transfer at a lower latency and cost compared to the public internet. To perform a backup copy to an AWS VTL gateway, the backup infrastructure must contain the following components:

- Source ESXi host(s) of the VMware Cloud on AWS
- VMware to AWS ENI Network tunnel
- Veeam Backup Server
- Veeam Backup Proxy
- Veeam Backup Repository: a Linux-based EC2 instance in Amazon AWS
- AWS Storage Gateway running in VTL mode for mounting to a Windows server as a tape library

Note: The VTL gateway can be placed in either VMware Cloud on AWS SDDC or natively on EC2



Note: This is a high-level overview and there are many design options available for placing the storage gateway, as well as the S3/Glacier region locations. When designing your secondary copy locations, you will need to take redundancy, location, costs and needs into consideration to plan the best design for the intended use case.

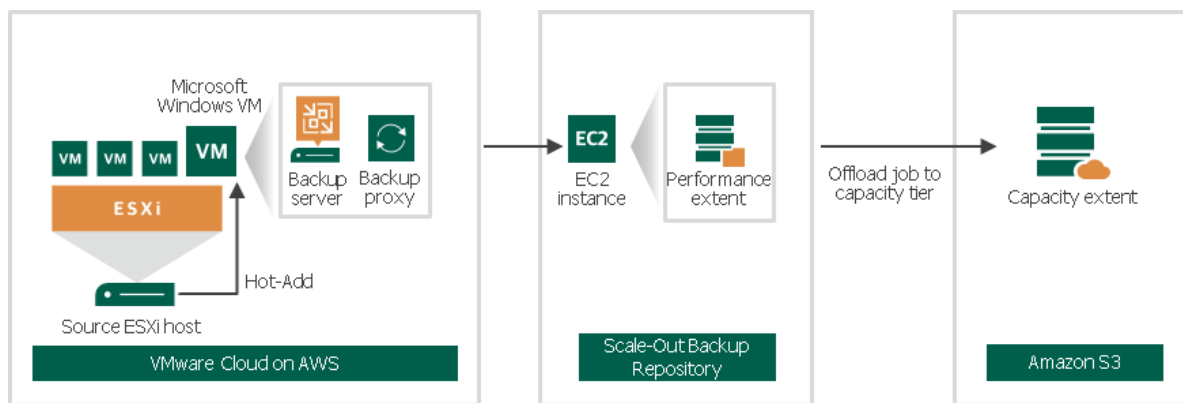
Deployment scenarios for capacity tier

If you have a scale-out backup repository with a capacity tier option configured, you can transfer your backups to the capacity tier for long-term storage. To do it, you can leverage Veeam capacity tier copy mode.

Note that capacity tier is available only as part of scale-out backup repository. For more information on capacity tier, see **capacity tier**.

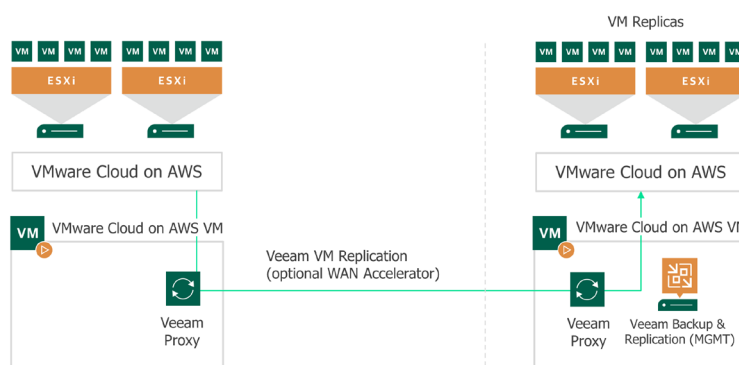
To transfer backup files to the capacity tier, the backup infrastructure must contain the following components:

- Source ESXi host
- Veeam Backup Server
- Veeam Backup Proxy
- Veeam Backup Repository: an EC2 instance in AWS
- A configured scale-out backup repository with object storage added as a capacity extent



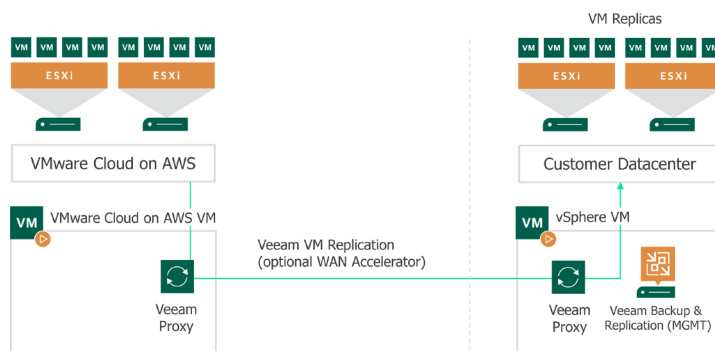
Deployment scenarios for disaster recovery for another geography on VMware Cloud on AWS

A customer can use Veeam VM replication for disaster recovery to replicate the VMs to another VMware Cloud on AWS in another supported region.



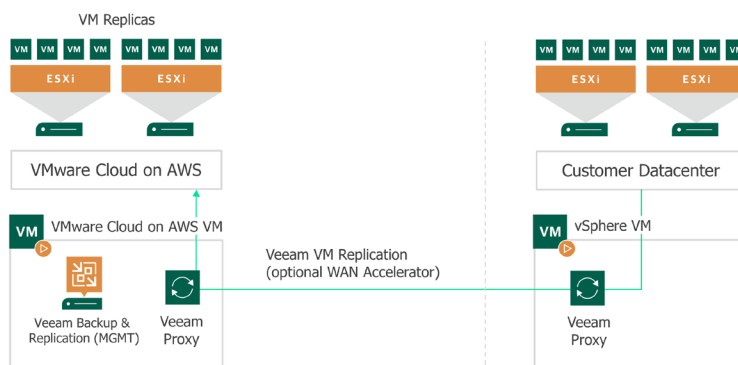
Deployment scenarios for disaster recovery on a customer datacenter

A customer can use Veeam VM replication for disaster recovery to replicate the VMs to their own VMware-based data center.



Deployment scenarios for VMware Cloud on AWS as a disaster recovery site

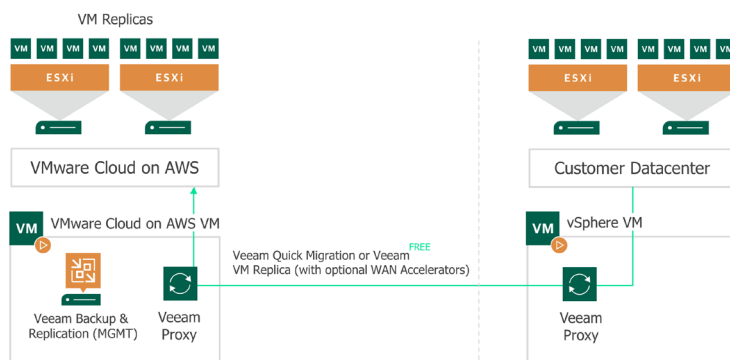
A customer can use Veeam VM replication for disaster recovery to replicate their own VMware-based data center to VMware Cloud on AWS.



Deployment scenarios for VM migration to VMware Cloud on AWS

A customer can use Veeam quick migration to migrate workloads from their VMware-based data center to the cloud (possible with Veeam Backup & Replication Community Edition).

Veeam VM replica can be used to replicate VMs to the cloud in the background for a controlled migration at a specific point in time.



System requirements

To perform data protection and disaster recovery tasks in VMware Cloud on AWS, consider the following recommendations and requirements on the backup infrastructure deployment:

- **Backup server:** It is recommended to deploy the Veeam backup server in the VMware Cloud on AWS environment. The machine must run Microsoft Windows.
- **Backup proxy:** You must deploy a backup proxy in the VMware Cloud on AWS environment. The machine must run Microsoft Windows. You can assign the role of the backup proxy to a dedicated VM or to the backup server. To provide sufficient resources, deploy at least one backup proxy per each SDDC cluster in the VMware Cloud on AWS. This is required for VMware Cloud on AWS specific Hot Add processing.
- **Backup repository:** It is recommended to use a backup repository created outside of the VMware Cloud on AWS environment, for example, on the Amazon EC2 instance. This type of deployment allows for efficient data transfer over the high-throughput, low-latency ENI connection used by VMware to communicate with AWS. Alternatively, you can store backups on a Veeam backup repository in the on-premises VMware environment.
- **Object Repository:** It is recommended to use an object repository for use with a scale-out backup repository to send secondary copies of the backup data to AmazonS3.

*Note that in this scenario you may incur a charge for outbound data transfer for the traffic from VMware Cloud on AWS to the internet.

- **Cloud Connect or AWS Storage Gateway (VTL mode):** It is imperative to maintain the 3-2-1 Rule for data availability and durability. Leveraging either the Veeam Cloud Connect or the AWS storage gateway in VTL mode to be able to land secondary copies of the data to another location is recommended.

*Note that in the Cloud Connect scenario you may incur a charge for outbound data transfer for the traffic from VMware Cloud on AWS to the internet.

Configuration

To deploy Veeam in VMware Cloud on AWS, first define the workflow processes. Once workflow processes are defined, review in detail how to achieve each task. The steps in this section will include:

- Provision SDDC in VMware Cloud on AWS
- Configure firewall rules for SDDC
- Deploy Veeam Backup & Replication server in SDDC
- Configure firewall rules for Veeam
- Deploy the Veeam repository server in EC2
- Test configuration

Provision SDDC in VMware Cloud on AWS

The first step is to deploy an SDDC in VMware Cloud on AWS from the console. For details on how to perform this please reference the [VMware docs site](#).

The [main VMware docs site for VMware Cloud on AWS](#) can be found here:

- <https://docs.vmware.com/en/VMware-Cloud-on-AWS/>

About this task

During the SDDC creation, you connect your SDDC to your AWS account and select a VPC and subnet within that account. Using a CloudFormation template, VMware Cloud on AWS creates an Elastic Network Interface (ENI), allowing for high throughput, low latency access to native AWS services and allowing your SDDC to communicate without needing to route traffic through the internet gateway. There is a one-to-one relationship between SDDCs and a customer AWS account.

Prerequisites

- Ensure that you have an AWS account before you create an SDDC. The VPC subnet you intend to connect should be in the same region that you plan to use for your SDDC. It should be noted that you will have the option to create a new VPC subnet in your AWS account during service onboarding.
- Create an appropriate subnet with at least 64 IP addresses (a /26 CIDR block) in each availability zone (AZ) in your VPC. The IP address range of this subnet must not overlap with the IP Address range 192.168.1.0/24, which is reserved for the default compute gateway logical network of your SDDC.

Deploy the SDDC following VMware Cloud on AWS Product Documentation referenced above.

Wait for the VMware SDDC deployment to complete.

Once the SDDC has been deployed you can now begin the process of deploying Veeam in the SDDC.

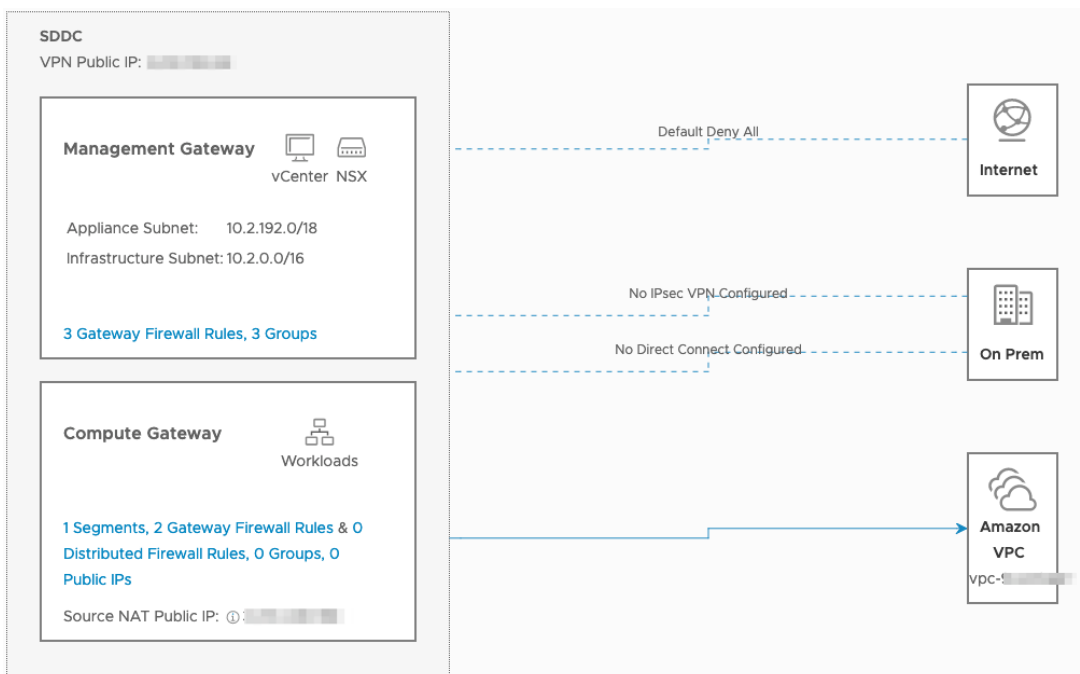
Configure firewall rules

Prior to deploying the Veeam server, the firewall rules will need to be added for proper communication. By default, the firewall for the management gateway is set to deny all inbound and outbound traffic. Add additional firewall rules to allow traffic as needed.

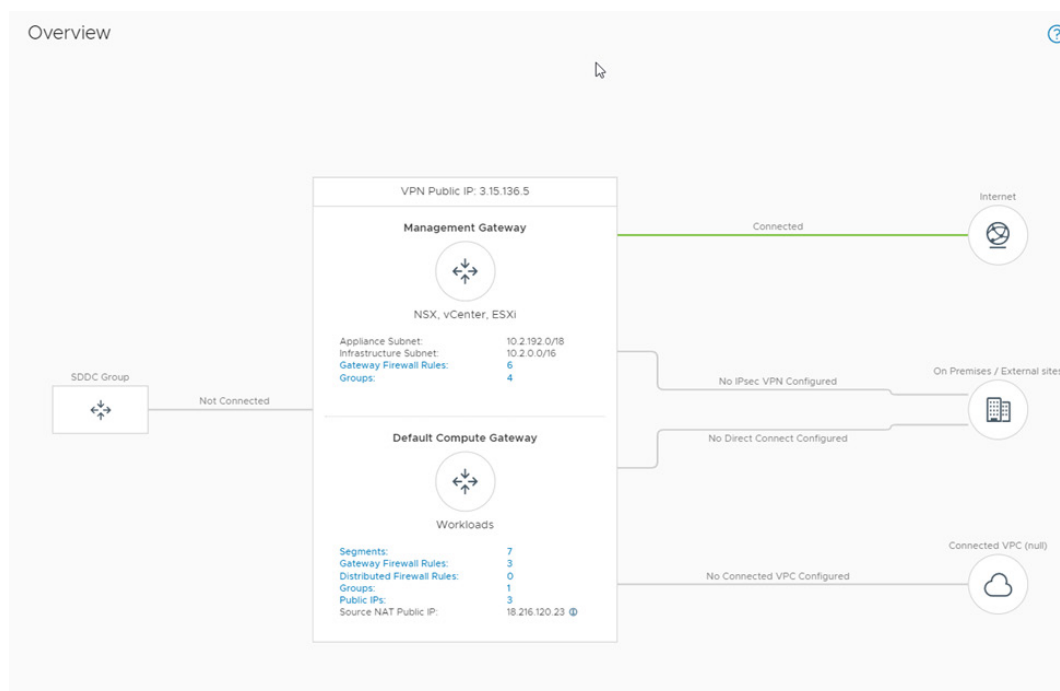
About this task

If you have configured a management gateway VPN, you can use the Firewall Rules Accelerator to create the firewall rules necessary for communication over the VPN.

Note: To access the vCenter server in your SDDC, you must set a firewall rule to allow traffic to the vCenter server. When access to vCenter server is blocked, the topology diagram on the Network tab shows a dotted line between the internet and the management gateway.



After you have added a firewall rule to allow access to the vCenter server, the diagram shows a solid line between the internet and the management gateway.



Procedure

1. Log in to the VMWONAWS Console at <https://vmc.vmware.com>.
2. Click **View Details** on the SDDC card.
3. Click **Networking & Security**.
4. Under **Security** – click **Gateway Firewall**, click **Management Gateway**.
5. Click **Add New Rule**.
6. Enter the rule parameters.

Option	Description
Rule name	Enter a descriptive name for the rule.
Action	The only action available for management gateway firewall rules is Allow.
Source	Enter or select one of the following options for the source: <ul style="list-style-type: none"> • An IP address, IP address range or any to allow traffic from that address or address range. • vCenter to allow traffic from your SDDC's vCenter server. • ESXi to allow traffic from your SDDC's ESXi management. • NSX Manager to allow traffic from your SDDC's NSX Management.

Option	Description
Destination	<p>Enter or select one of the following options for the destination:</p> <ul style="list-style-type: none"> An IP address, IP address range, or any to allow traffic to that address or address range. vCenter to allow traffic to your SDDC's vCenter server. ESXi Management Only to allow traffic to your SDDC's ESXi management. NSX Manager to allow traffic from your SDDC's NSX Management.
Services	<p>Select one of the following to apply the rule to:</p> <ul style="list-style-type: none"> Any (All traffic) ICMP (All ICMP) HTTPS (TCP 443) – applies only to the vCenter server as a destination SSO (TCP 7444) – applies only to the vCenter server as a destination

Use the up and down arrow icons to change the order of the firewall rules.

***Note:** Firewall rules are applied in order from top to bottom.

Example

The following graphic shows an example firewall rule that allows all traffic to reach the vCenter server from a particular IP address.


	Name	Sources	Destinations	Services	Action	
<input type="checkbox"/>	Veeam - vCenter	Veeam	vCenter	HTTPS (TCP 443) SSO (TCP 7444) ICMP (ALL ICMP)	Allow	<input checked="" type="checkbox"/>

See [Example Management Gateway Firewall Rules](#) for further information regarding specific use case firewall rules.

The **Open vCenter** button for your SDDC assists you in connecting to the vCenter server in several ways. In addition to the **OPEN VCENTER** button, the **Settings** tab for your SDDC provides connection and authentication details for connecting to the vCenter server with the API Explorer and PowerCLI.

The procedures for selecting a method are described below, as well as at the following link: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-C057DF7D-8016-45C4-AE12-56490E013F95.html>

Select a method for connecting to your SDDC's vCenter server.

Option	Description
Connect using the vSphere Client	Click the link under vSphere Client (HTML5). This connection method is identical to the OPEN VCENTER button.
Connect to the API Explorer	Click the link under vCenter Server API Explorer.
Connect using PowerCLI	The cmdlet for connecting is shown under PowerCLI Connect. Click  to copy the cmdlet to the clipboard.

Deploy the Veeam Backup & Replication server in SDDC

Now that the SDDC has been created and firewall rules have been added, you may begin installation of the Veeam server.

Implementation step 1. Veeam Backup & Replication







1. Use a new Windows server and install Veeam Backup & Replication 9.5 Update 4 or newer if you do not have a Veeam backup server. The server can run within any VMware Cloud on AWS SDDC, Amazon EC2 instance or on-premises environments.
2. Add DNS network settings so that this server can resolve internet DNS names.
3. Check the below information carefully for any known limitations and configuration steps before you proceed.

Implementation step 2. VMware Cloud on AWS

Firewall configuration for vCenter connection for Veeam

The Veeam Backup & Replication server and Veeam proxy server should be connected to the VMware vCenter using HTTPS through TCP port 443. In VMware Cloud on AWS, there is no need to open ports to the ESXi hosts itself. As the vCenter server in VMware Cloud on AWS is on another network (Management Network) by design, you need to implement a VPN tunnel to it or configure the following firewall settings:

1. Open Port TCP 443 from the backup server and proxy server to the predefined vCenter object on the compute network.

	<input type="checkbox"/>	Veeam and Proxies	1015				A
	<input type="checkbox"/>	Default VTI Rule	1012	Any	Any	Any	V
	<input type="checkbox"/>	Default Uplink Rule		Any	Any	Any	A

Implementation step 3. Add vCenter

Add vCenter to the Veeam console as described here: https://helpcenter.veeam.com/docs/backup/vsphere/add_vmware_server.html?ver=110

1. Create a vCenter user with required rights (Active Directory linked mode) https://helpcenter.veeam.com/docs/backup/vsphere/required_permissions.html?ver=110 or use the **cloudadmin@vmc.local** user.
2. When adding a vCenter server, specify the fully qualified domain name (FQDN) that ends with **vmwarevmc.com** or **vmc.vmware.com** (depending on the URL shown in the VMWONAWS interface for the vCenter).

Usage of the local connection for customers with VMware NSX-t

NSX-t allows VMC customers to directly access the management network over the built-in firewall. TCP Port 443 needs to be opened from all Veeam backup and Veeam proxy servers as a source, with the vCenter internal IP as a target.

- a) Configure DNS entry of the vCenter for local IP address usage.

Go to your **SDDC Management -> Settings -> vCenter FQDN** and select the **Private vCenter IP** address.

The screenshot shows the Veeam SDDC Management console with the 'Settings' tab selected. Under 'vCenter Information', the 'vCenter FQDN' section is expanded. It displays the 'vCenter FQDN' as 'https://vcenter.sddc-54-184-129-10.vmwarevmc.com/'. Below this, the 'Resolution Address' dropdown is open, showing 'Public IP: 54.184.129.10' and 'Private IP: 10.2.224.4'. The 'Private IP' option is selected. The 'Public IP' is 54.184.129.10 and the 'Private IP' is 10.2.224.4. There are 'SAVE' and 'CANCEL' buttons at the bottom of the section.

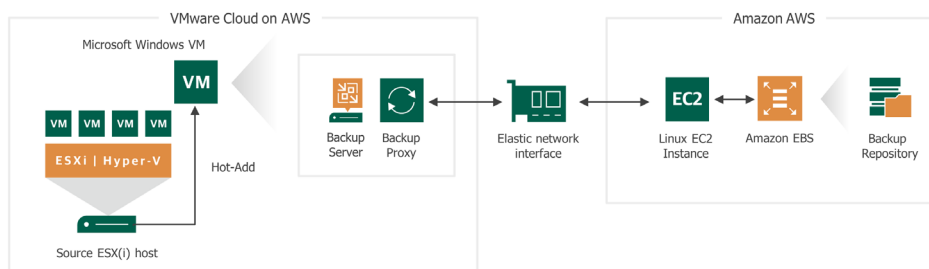
Hint: If you configure the vCenter DNS record for the internal IP address, you will lose the VMware Cloud on AWS connection from the Backup & Replication server outside of VMware Cloud on AWS. You can use the local hosts file or any other DNS method to resolve the vCenter FQDN with the public IP address on the Veeam server outside of VMC. Optionally, use the public IP address for the VMware Cloud on AWS internal and external Veeam server.

Implementation step 4. Add Veeam proxy

For any VMware Cloud on AWS SDDC cluster, deploy at least one Veeam proxy server to be able to process **Hot Add/Virtual Appliance Backup Mode**. The Backup & Replication server itself can be used when installed at the SDDC cluster (proxy preinstalled). Please look at the Veeam documentation for details: https://helpcenter.veeam.com/docs/backup/vsphere/add_vmware_proxy.html?ver=110

Implementation step 5. Add Veeam repository

VMware Cloud on AWS uses vSAN as primary VM storage. It is not recommended to use that disk for production workloads and backups due to a variety of factors including cost. As a result, an external backup device is recommended. Depending on the use case, there are several ways to achieve this with different economic factors. The example below provides further detail of how an Amazon EC2 Linux instance (e.g. EC2 C4 Instance with EBS ST1 volumes) may be used as a backup target over the VMware Cloud on AWS integrated ENI network connection:



Note: As mentioned previously, this reference design is for illustration purposes. During planning, please be sure to account for secondary copies of the data. For example, you could leverage EFS, VTL, Cloud Connect, etc.

To connect the EC2 Server(s) used for Veeam Repositories the following firewall configuration is needed:

1. On the Compute Gateway:

- a. Open TCP 22 (SSH) port from the Veeam Backup Server and Veeam proxy server to the Amazon VPC where the EC2 Server was installed. You can also define the exact IP addresses of the repository server as Destination.
- b. Open TCP 2500-5000 ports for Veeam Data Transport in both directions for same servers. It is recommended to use the VMware Cloud on AWS integrated high throughput/low latency ENI network connection to avoid additional costs.

Management Gateway 4 Rules	<div>REVERT PUBLISH</div> <div>Q Search</div>						
Compute Gateway 2 Rules							
	Name	Source	Destination	Services	Action	Applied To	Logging
	Veeam Repository SSH	Veeam Backup Server and Veeam Proxy Server	Connected VPC Prefixes	SSH	Allow	All Uplinks	Disabled
	Veeam Transport (In)	Connected VPC Prefixes	Veeam Backup Server and Veeam Proxy Server	Veeam Transport TCP 2500-5000	Allow	All Uplinks	Disabled
	Veeam Transport (Out)	Veeam Backup Server and Veeam Proxy Server	Connected VPC Prefixes	Veeam Transport TCP 2500-5000	Allow	All Uplinks	Disabled

Open the same ports on the Inbound Firewall of the Amazon EC2 server used as a repository server.

Implementation step 6. Add secondary backup target

It is suggested to create a backup copy to an additional place. Depending on the use case, there are several ways to achieve this with different performance and cost metrics. Listed below are just a few of the ways that the following technologies can be used:

1. Veeam Backup Copy Job to a second Amazon EC2 instance can be used as an additional repository. The second Amazon EC2 instance can be placed on another AWS Availability zone or AWS region.
2. AWS Storage Gateway Software in VTL mode can be used to emulate a tape library to write data to Amazon S3. Veeam Backup to Tape Jobs can be used with it. For details, see: <https://www.veeam.com/wp-using-aws-vtl-gateway-deployment-guide.html>
3. Veeam Backup Copy Job to on-premises or Veeam Cloud Connect. There is no special configuration needed for this use case, besides network and firewall connections. For standard repository usage on-premises, it is recommended to create a VPN tunnel from VMware Cloud on AWS to the on-premises data center. This may be performed using the VMC integrated VPN functionality, by Veeam PN or a third party.
4. Use Amazon EFS or FXs to send backup copies for a secondary repository.

Note: The use of a Cloud Connect use case may incur outbound data transfer charges. Please evaluate the advantages and disadvantages of each when planning your architecture as costs may vary.

Additional scenarios

1. VMware Cloud on AWS used as a restore target.
 - a. Implementation steps 1-4 are needed.
2. Veeam VM replication.
 - a. Implementation steps 1-5 are needed. The repository server (when NOT used for backups) can run within the VMware Cloud on AWS SDDC to store the Veeam replication data. On-premises to VMWONAWS, VMWONAWS to VMWONAWS and VMWONAWS to on-premises are possible. Usage of Veeam Disaster Recovery Orchestrator is possible in specific scenarios, see the Veeam Disaster Recovery Orchestrator deployment guide: <https://helpcenter.veeam.com/docs/vao/userguide/welcome.html?ver=40>.

Additional information for the rollout:

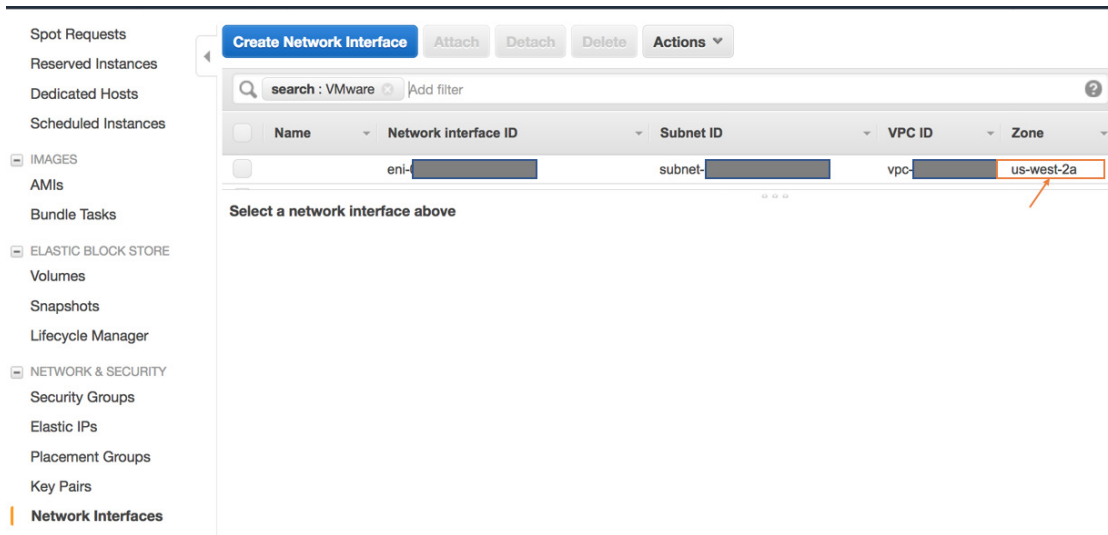
Amazon AWS configuration details and background information:

Customer account AWS configuration details:

This section covers recommendations for the AWS account VPC, in areas of VPC subnet, route table, security group, network ACL, AWS Identity Access Management (IAM), Amazon EC2, Amazon Elastic Block Store (EBS), Amazon Elastic File Service (EFS) and AWS Storage Gateway.

VPC

1. Deploy the native instance in the same subnet or another subnet in the same availability zone as the VMware SDDC ESXi hosts. Ensure the logical network where Veeam Backup Server and proxy VMs are connected to have proper routes to/from SDDC:



The figure above shows how to use the AWS Management Console to identify the availability zone associated with the ENIs provisioned as part of VMware service onboarding.

```
#aws ec2 describe-network-interfaces | grep -i "vmware" -A 17
"Description": "VMware VMC Interface DO NOT USE - 6",
  "NetworkInterfaceId": "eni-123456789101112",
  ...
  "AvailabilityZone": "us-west-2a",
```

The figure above shows how to use AWS CLI to identify the availability zone associated with the ENIs provisioned as part of VMware service onboarding.

Note: The main route table is updated automatically when a new logical network is created within the VMware Cloud on AWS environment. If a given subnet is not explicitly associated with the main route table, the routes in the main route table will be used for the subnet. If the EC2 instance serving as a Veeam backup repository is deployed in a subnet associated with non-main route table, then ensure the logical network for the Veeam backup and proxy server is added to the associated route table.

Destination	Target
10.60.0.0/16	Local
10.70.10.0/24	eni-123456789101112

VMware SDDC Logical Network ENI attached to VMware ESXi host

2. It's recommended to deploy the Amazon EC2 instance serving as a backup repository into a private VPC subnet. Outbound internet access is required to obtain necessary software for backup repository configuration or patching can be enabled through the NAT Gateway service, or a dedicated NAT Gateway deployed in a public VPC subnet.

Example configuration:

The NAT Gateway deployed in a public VPC subnet with assigned Elastic IP address

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Create NAT Gateway

Actions

Filter by tags and attributes or search by keyword

1 to 3 of 3

	Name	NAT Gateway ID	Status	Status Message	Elastic IP Address	Private IP Address
<input checked="" type="checkbox"/>		nat-076ac55e60f2...	available	-	52.33.54.179	10.60.2.156
<input type="checkbox"/>		nat-04e5fc9cb7e3...	available	-	34.218.211.100	10.60.1.75
<input type="checkbox"/>		nat-04c218a4c7ec...	available	-	52.24.43.94	10.60.3.70

NAT Gateway: nat-076ac55e60f2960f8

Details

Monitoring

Tags

NAT Gateway ID

nat-076ac55e60f2960f8

Status

available

Status Message

-

Elastic IP Address

52.33.54.179

Private IP Address

10.60.2.156

Network Interface ID

eni-dbecd8ec

VPC

vpc-071f6d070e9d72a88 | VPC-network-config

Subnet

subnet-0c24dae1a86f9e86 | Public subnet 2

Created

March 15, 2018 at 12:17:09 PM UTC-7

Deleted

-

A private subnet routing table entry for outbound internet traffic to go through the NAT gateway

rtb-047160432cab855e4 | Private subnet 1A

Summary

Routes

Subnet Associations

Route Propagation

Tags

Edit

View: All rules

Destination	Target	Status	Propagated
10.60.0.0/16	local	Active	No
0.0.0.0/0	nat-04e5fc9cb7e335b5a	Active	No

3. Security group for the EC2 instance serving as a Veeam backup repository, allowing TCP traffic over specific ports from Veeam proxy/backup server running in VMware SDDC:

Note: You can further refine this to be more granular, so that only the Veeam VM can communicate with the EC2 instance.

sg-0fb2289b244b6d783 | SDDC ENI

Summary

Inbound Rules

Outbound Rules

Tags

Edit

Type	Protocol	Port Range	Source	Description
ALL Traffic	ALL	ALL	10.70.0.0/16	SDDCs

4. Customers can also leverage Network ACL as an additional layer of control to allow inbound and outbound traffic at individual subnet level:

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

Cancel

Save

View: All rules

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	10.70.0.0/16	ALLOW

View: All rules

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	ALL Traffic	ALL	ALL	10.70.0.0/16	ALLOW

5. It's recommended to enable VPC flow logs for the EC2 instance's private subnet, so traffic information can be captured for security monitoring and troubleshooting purposes. As a start, enable VPC flow logs for the ENI attached to the Amazon EC2 instance serving as the backup repository to capture all the traffic.

Create Flow Log

×

Flow logs enable you to capture IP traffic flow information for the network interfaces in your resources.

[Learn more about flow logs.](#)

Resources eni-

i

Filter* All

i

Role* flowlogsRole

i

If you have not setup IAM permissions for the destination CloudWatch Account you will need to do so to use Flow Logs. [Set Up Permissions](#)

ARN arn:aws:iam:::role/flowlogsRole

i

Destination Log Group* VMCbackup

i

*: Required

Cancel

Create Flow Log

Sample VPC Flow Logs captured for the ENI attached to the EC2 instance serving as a backup repository:

2 987654321012	eni-12345678910	<Source IP>	<Destination IP>	<Source port>	<Destination Port>	<Protocol ID>	<Packets>	<Start>	<End>	<action>	<Log status>
Account ID	ENI attached to backup repository instance									Accept or Reject	

IAM:

1. Do not use the root account to launch the EC2 instance. Instead, create a dedicated IAM user following the best practice of least privilege so the IAM user only has enough privilege to deploy the EC2 instance and all the necessary actions on the VPC specific settings.
2. Use certificate-based authentication for an EC2 backup repository.

Backup repository sizing recommendations

EC2 instance family/type:

- If Veeam Backup Jobs indicate storage as the bottleneck, then consider using EBS Optimized instance for best performance
- It is also important to understand how EBS volume sizing can determine its baseline performance. Please refer to the following link for details around this: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html>
- Enable auto recovery for the instance, so the instance impaired due to failure of underlying hardware can be recovered automatically. Note the [supported EC2 instance type](#) and ensure the instance type selected as the backup repository can support auto recovery

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☒ **Send a notification to:** VMC_backup_VM_failure [cancel](#)

With these recipients: [redacted]@amazon.com

☒ **Take the action:**

- ☒ Recover this instance ⓘ
- ☐ Stop this instance ⓘ
- ☐ Terminate this instance ⓘ
- ☐ Reboot this instance ⓘ

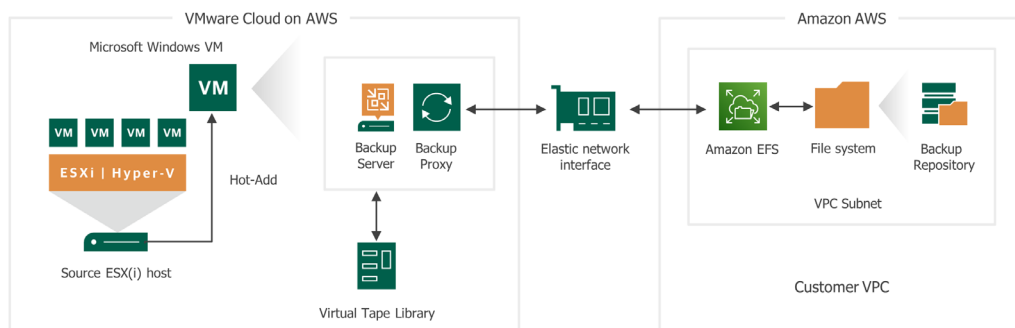
Whenever: Maximum ⓘ of Status Check Failed (System)

Is: Count

For at least: consecutive period(s) of ⓘ

Name of alarm: VMCbackup [redacted]

Consider using a managed service to eliminate instance management. One option is to leverage Amazon EFS service to serve as the backup repository.



The figure shows Veeam backup using Amazon EFS as primary repository, with the backup copy job sent to AWS Storage Gateway (VTL mode) to comply with the 3-2-1 Rule best practices.

References

Veeam KB entry for VMware Cloud on AWS compatibility: <https://www.veeam.com/kb2414>

VMware documentation for VMware Cloud on AWS: <https://docs.vmware.com/en/VMware-Cloud-on-AWS/services/com.vmware.vmc-aws.getting-started/GUID-3D741363-F66A-4CF9-80EA-AA2866D1834E.html>

Veeam help center for VMware Cloud on AWS: https://helpcenter.veeam.com/docs/backup/vsphere/vmware_cloud_aws.html

VMware KB entry for Veeam Backup & Replication with VMware Cloud on AWS: <https://kb.vmware.com/s/article/52533>

VMware Cloud on AWS — Resources: <https://aws.amazon.com/vmware/resources/>

About Veeam Software

Veeam® is the leader in backup solutions that deliver Cloud Data Management™. Veeam provides a single platform for modernizing backup, accelerating hybrid cloud and securing data. Veeam has 400,000+ customers worldwide, including 83% of the Fortune 500 and 69% of the Global 2,000. Veeam's 100% channel ecosystem includes global partners, as well as HPE, NetApp, Cisco and Lenovo as exclusive resellers. Veeam has offices in more than 30 countries. To learn more, visit <https://www.veeam.com/> or follow Veeam on Twitter @veeam.

veeam

NEW

V11

Eliminate Data Loss
Eliminate Ransomware

#1 Backup and Recovery



Try now:

<https://www.veeam.com/backup-replication-virtual-physical-cloud.html>